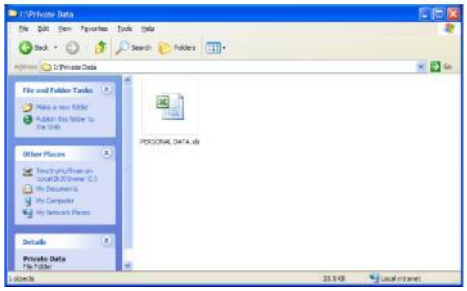
How to... **ENCRYPT/DECRYPT USING AXCRYPT**

These instructions assume that you have already installed AxCrypt software on your computer. If you have not already installed the software, please refer to instructions named “How to... INSTALL AXCRYPT SOFTWARE”.

To encrypt a file, browse to the location of the file.

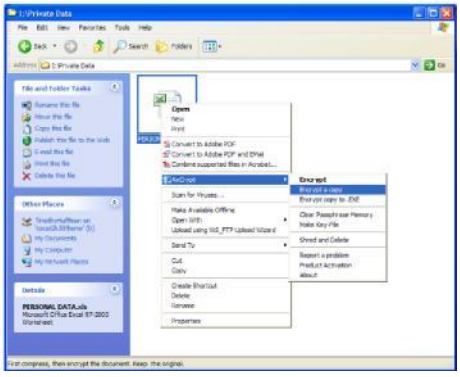


Right-click on the file to be encrypted. Go down the menu to AxCrypt to expand the encryption menu. To encrypt the file, one of the first 3 choices must be made.

“Encrypt” encrypts the selected file. If this is the only copy of the file, this copy will be encrypted.

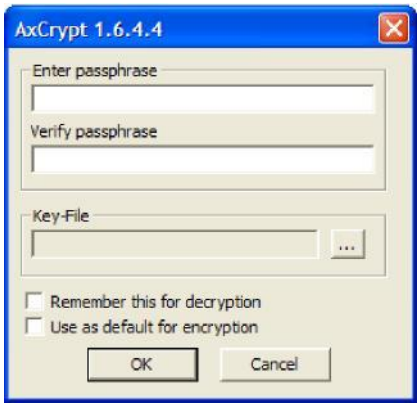
“Encrypt a copy” creates a new encrypted copy of the file while leaving the original file in its current state.

“Encrypt copy to .EXE” will create a copy of the file like above, but the new encrypted version will be contained in a self-extracting format for users that do not have AxCrypt installed.



For the purpose of this training, select “Encrypt a copy”. For additional training, please refer to the AxCrypt instructions and references available at www.axantum.com/**AxCrypt**/.

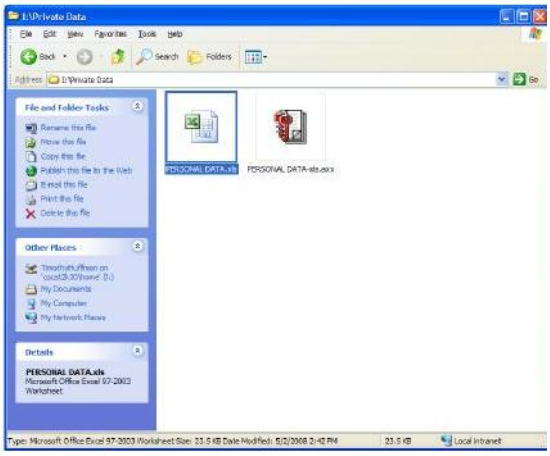
“Encrypt a copy” displays the encryption dialog box. In the “Enter passphrase” and “Verify passphrase” boxes, enter the password required for users to open the file once encrypted.




To reach HIPPA-required 128-bit encryption, a Key-File must be specified. To specify a key-file, click the ellipsis (“...”) button to browse to the key file. *(In this example, the key file is named ‘dss-key.txt’. To meet 128-bit encryption levels, requirements for file length and complexity are necessary. However, these requirements are beyond this training. To find out more, refer to whitepapers at www.axantum.com/**AxCrypt**/.)* Browse to the folder that contains the specified file key (received from DSS), select the file, and then click “Open”. The file path should display in the key-file box.

How to... **ENCRYPT/DECRYPT USING AXCRYPT**

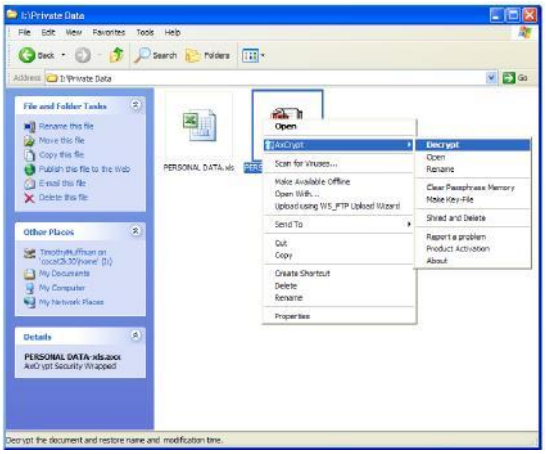
*(If this is the primary key file used for encryption, the checkbox for "Remember this for decryption" will maintain a reference to the key file for later use. If this key file will be maintained for use later for additional encryption, "Use as default for encryption" will maintain a reference to the key file for future encryptions.)*



The file location should now display an additional file (with the original file name and an *.axx extension), the encrypted version of the selected file initially selected.

The encrypted file can be safely sent via email or other method to persons that possess the key file and password. *(At no time should an encrypted file and the key file be sent together. While it is possible to send the password along with an encrypted file that uses a key-file, this practice is also not recommended.*
*Also, after you receive a key-file from DSS, all documents to/from DSS should use the same key-file until a new key-file is created to replace an old key-file.)*

**IMPORTANT:** After creating a password to encrypt a file, it is your responsibility to track the password. There is **NO** recovery of documents from forgotten passwords.

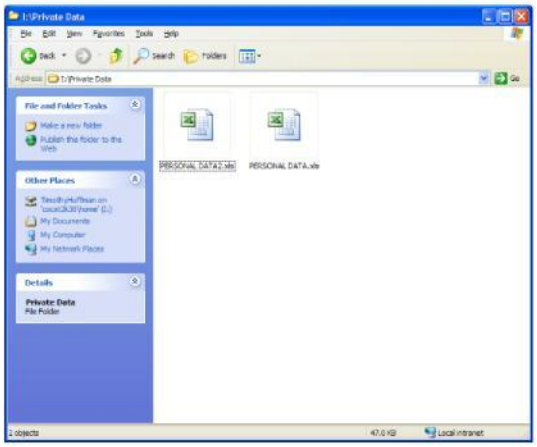


To decrypt an AxCrypt file, right-click on the file, then navigate the the AxCrpyt menu to select "Decrypt". *(For files sent via email, the file must be saved onto your computer and out of the email program to display the appropriate menu.)*

If you selected for the program to remember your key-file and passphrase, the program will decrypt the file to the current location.

If you did not choose the save the passphrase and key-file, or if the passphrase and key-file are not correct for the file, you will be prompted to enter the necessary data.


Enter the password. Select the proper key-file for the file, then click “OK”.



The document should decrypt to its current location.

For more information regarding AxCrypt and its use, please refer to the AxCrypt homepage: www.axantum.com/**AxCrypt**/ Technical specifications and whitepapers are available for reference regarding this open-source encryption software.